Post-Quantum Digital Signing for PDF Documents

Teik Guan Tan, Shi Hong Choy
pQCee

Hsien Hui Tong, Terry Boon Jay Tan, Muhammad Zulhilmi bin Miswadi
SGInnovate

Introduction

Digital Portable Document Format (PDF) documents are used widely by both businesses and individuals as the electronic equivalent of paper documents. There are probably more than one trillion PDF documents in existence today, and this number will continue to grow. The contents in these documents may range from:

- **Business contracts.** e.g. Non-disclosure agreements, employee hiring contracts, rental agreements, sales orders, trade documentation;
- **Statutory documents.** e.g. electronic visas, certificates of eligibility, qualification certificates, court letters;
- **Records of storage** e.g. Scanned paper documents, e-printed emails.

Many of these PDF documents have long-dated validity and their proof of authenticity of these documents are may required for over 10 to 25 years, depending on their contents and value they represent. Current public key digital signing techniques are inadequate to ensure the integrity and authenticity of these documents due to the threat that quantum computers bring.

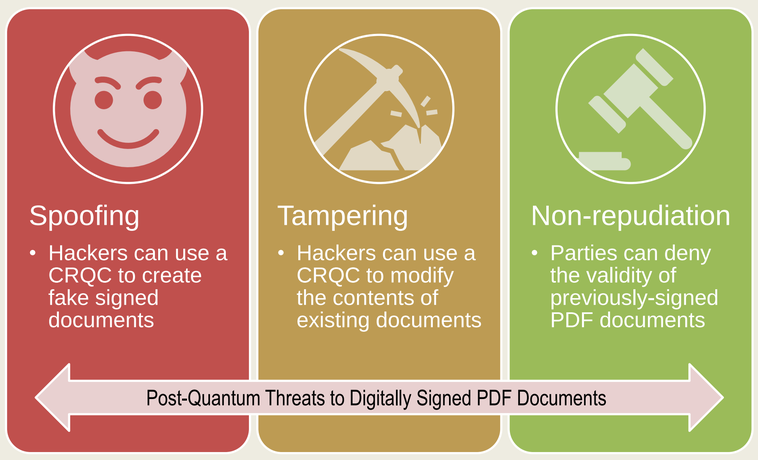
In this paper, we demonstrate how we can apply post-quantum cryptography (PQC) to enhance the protection of PDF documents such that the proof of authenticity remains secure even against quantum computers, while maintaining the backwards-compatibility to existing systems and applications so that business operations are not disrupted.

Post-Quantum Threat to PDF Documents

Cryptographically-relevant quantum computers (CRQC) are expected to be available within the next 5 to 10 years. With CRQCs, a malicious actor will be able to exploit the cryptographic weakness in existing classical public key algorithms such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Digital Signing Algorithm (ECDSA) and create fake digital signatures that are not discernable from actual valid signatures.

The result is that attackers will be able to spoof the identities of the counterparties in business agreements and forge or modify agreements to disprove current contracts. Once evidence of tampering exists, the authenticity of the PDF documents and agreements will be brought into question, and this can adversely affect each parties' ability to enforce them in the legal courts.

On the other hand, valid digitally-signed PDF documents will lack the non-repudiation properties if one of the signing parties want to renege on the agreement and claim that the previously-signed document is, in fact, faked by a CRQC.



These threats will likely bring about more disruption to the existing course of business, a general loss of trust in business arrangements, increased legal and compliance fees, and an overall prolonged delay for dispute resolution.

Post-Quantum Migration Requirements

The security of existing digitally-signed PDF documents therefore needs to be strengthened. This involves the use of PQC digital signing algorithms which are resistant to CRQC attacks.

In addition, there are business requirements to ensure the smooth migration to quantum-safety. These are:

- **Backwards-compatibility**: The quantum-safe PDF documents will need to be compatible on existing PDF readers (e.g. Adobe Acrobat)
- **Cryptographic-agility**: The quantum-safe PDF documents should be able to support new/future cryptographic standards.
- **Data Privacy**: When enhancing the protection of existing signed PDF documents, the contents of the PDF documents should not be exposed outside the organization

Post-Quantum Digital Signing

We chose to implement pQCee's patent-pending Signature Pre-image Proof (SPP) for ECDSA [1] using the RFC 3161 Time Stamp Protocol (TSP) [2] as the post-quantum digital signing technique to protect existing PDF documents. This is because of:

- **Cryptographic Compatibility**
  Existing Adobe Acrobat PDF readers only support the verification of classical digital signing algorithms (RSA and ECDSA). The use of new PQC algorithms (e.g. MLDSA or SLHDSA) will require an upgrade of all PDF readers which is beyond the scope of the project. Instead, SPP is able to retain the use of ECDSA, while making the PDF document quantum-safe. The use of SPP will also not exclude the use of new PQC algorithms in the future to protect the existing PDF document

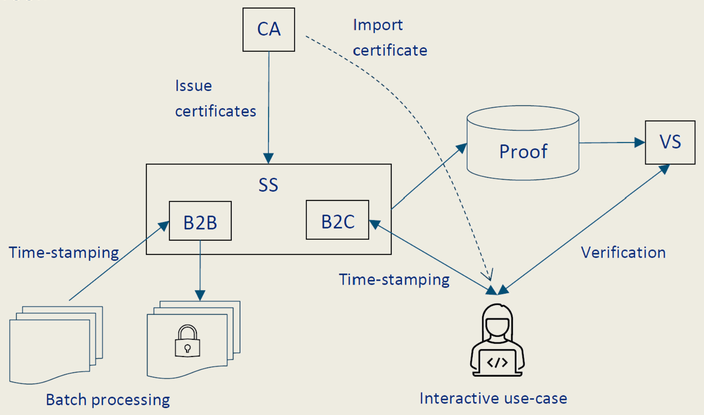
- **Privacy Preserving**
  Existing Adobe Acrobat PDF readers have built-in support for TSP to digitally sign PDF documents. During the signing process,
  a) A cryptographic hash of the PDF document is created by the PDF reader.
  b) A signing request containing only the hash is sent to the TSP digital signing service.
  c) The TSP digital signing service will return a signature containing the hash along with a time-stamp of the time of signing.
  d) The PDF reader will embed the time-stamp signature into the PDF document automatically.

  Such a setup will ensure both data privacy of the PDF document contents as well as usability of the TSP digital signing service for businesses and individuals.

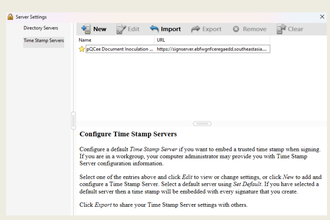
InoQulate Time Stamping Service

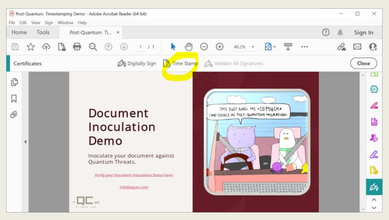
InoQulate is available as an offering on the Azure Marketplace [3].

We implemented InoQulate time-stamping service that uses SPP-ECDSA to sign incoming TSP requests. We used a simple 2-tier certificate hierarchy where the Root Certificate Authority (CA) will issue a time-stamping server certificate for the signing server (SS). We also included a verification server (VS) to allow users to check the SPP proof.



The service is designed to support both signing in interactive and batch mode.





When using in interactive mode, users will do a one-time configuration of a Time Stamp Server in Adobe Acrobat. Once done, users can now use the "More Tools→Certificates→Time Stamp" functionality to request a SPP-ECDSA signature via the RFC3161 TSP on the entire document.

Batch Mode (B2B)

In batch mode, the Signing Server can be pre-configured to retrieve PDF documents from a pre-determined source location for document time-stamping. This configuration is suitable for a locally-deployed inoQulate Time Stamping Service.

The signing server will then be configured at regular intervals to (i) sign the documents; (ii) store the signed documents in a different repository; and (iii) generate a batch job report to the administrator.

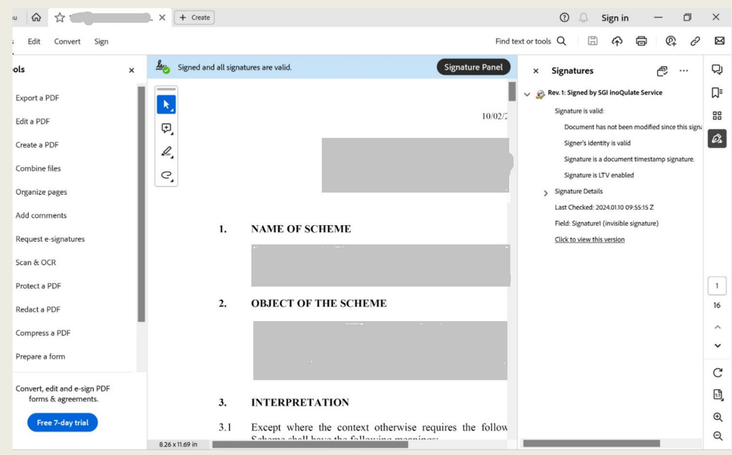
Pilot Deployment

The InoQulate Time Stamping Service is piloted by SGInnovate. A total of 43 documents were selected for the pilot based to their requirements for long-term archival.

The following work was carried out:

- Purchasing and initial configuration of inoQulate from the Azure Marketplace
- Provisioning, Installation and Configuration of inoQulate in SGInnovate's dedicated Private Cloud Sandbox environment
- Secure setup of Keys and Passwords for Certificate Authority and Signing Server by SGInnovate
- Batch execution of inoQulate timestamping of PDF documents
- Verification of timestamp signature and compatibility with Adobe Acrobat

The figure below shows a screenshot (with portions redacted) of an actual document signed by SGInnovate's InoQulate service and viewed from an Adobe Acrobat PDF reader.



We note that Adobe Acrobat is able to verify the SPP-ECDSA signature and treats the post-quantum timestamped document as valid.

Future work

The project has been successful in meeting both technical objectives (Post-Quantum digital signing) and business objectives (backwards compatibility, cryptographic agility, data privacy) to protect PDF documents against quantum threats.

We are on the next phase of the product development which includes:

- Support for NIST PQC FIPS204, FIPS205 algorithms.
- Support for native PDF signing and verification via Microsoft CNG API

Acknowledgements

This project is partially supported by Singapore's Talent, Innovation and Growth (TIG) Cybersecurity Industry Call for Innovation Grant 2023

This setup incorporates certain features that may be subject to claims in pQCee's patent-pending application (PCT WOWO2023080842).

References

[1] Tan, Teik Guan, and Jianying Zhou. "Layering quantum-resistance into classical digital signature algorithms." In Information Security: 24th International Conference, ISC 2021, Virtual Event, November 10–12, 2021, Proceedings 24, pp. 26-41. Springer International Publishing, 2021.

[2] Adams, Carlisle, Pat Cain, Denis Pinkas, and Robert Zuccherato. "RFC3161: Internet X. 509 public key infrastructure time-stamp protocol (TSP)." (2001).

[3] InoQulate is available at https://azuremarketplace.microsoft.com/en/marketplace/apps/pqceeptelltd1686816032301.pqcee-inoqulate-solution

Contact Information

Teik Guan Tan

pQCee Be . Quantum . Ready

Tel: +65 9746 9386
@tanteikg

Email: teikguan@pqcee.com
Web: www.pqcee.com